REMARKS/ARGUMENTS

Before this Amendment, claims 1, 2, 4-18, 20-27, 29-35 and 59 were examined. Claims 1, 5, 7, 15, 17, 18, 21, 22, and 25 are amended. No claims are presently added or canceled. Therefore, claims 1, 2, 4-18, 20-27, 29-35, and 59 remain present for examination, and claims 1, 17, 18, 21, 22, 25, and 29 are the independent claims. Support for the amendment may be found in the Specification (Original Application, p. 4, ll. 25-31).

The Office Action dated December 29, 2006 ("Office Action") rejected claims 1, 2, 4-17, 29-35 under 35 U.S.C. §103(a) as unpatentable over the cited portions of U.S. Patent 6,101,477 to Hohle et al. ("Hohle") in view of the cited portions of U.S. Patent 5,677,955 to Doggett ("Doggett") and further in view of the cited portions of U.S. Patent 6,304,223 to Hilton et al. ("Hilton"). The Office Action rejected claims 18, 20, and 22-28 under 35 U.S.C. §103(a) as unpatentable over the cited portions of U.S. Patent 6,226,744 to Murphy et al. ("Murphy") in view of Hilton and further in view of Doggett. The Office Action rejected claim 21 under 35 U.S.C. §103(a) as being unpatentable over Hohle in view of Murphy, further in view of Hilton and further in view of Doggett. Reconsideration is respectfully requested.

35 U.S.C. §103(a) Rejections, Dogett

The Office Action rejected independent claims 1, 17, 21, and 29 under 35 U.S.C. §103(a) as unpatentable over Hohle and various combinations of references cited above. Various embodiments of the present invention comprise systems or methods for establishing a secure communication link *between* a *smart card* and a *central computer system*, wherein the secure data is *passed through a smart card communication device* remote from the central computer system. To establish a *prima facie* case of obviousness, the prior art references must "teach or suggest all the claim limitations." MPEP §2143.

The cited references cannot be relied upon to teach or suggest the limitations of independent claims. Specifically, the references fail to teach 1) secured data formatted by the smart card to allow the central computer system to detect a modification to the secured data occurring during transmission beginning at the smart card, passing through a smart card communication device, and extending through to the remotely located central computer system,

as generally recited in claims 1, 17, 21, 22 or 29, or 2) a second set of secured data, the second set formatted by the central computer system to allow the smart card to detect a modification to the second set occurring during transmission beginning at the remote central computer system, passing through a smart card communication device, and extending to the smart card, as recited in claim 17, 18, and 25.

Although unclear, the Office now appears to rely on Doggett to teach these limitations; however, as will be explained in greater detail below, this reliance is not proper. In short, the claims specifically set forth a central computer system remote from the smart card and/or smart card communication device. However, the Office appears to equate the PCMCIA card of Doggett with the smart card of the claims (Office Action, p. 3, ll. 17-22; p. 9, ll. 1-14, p. 10, l. 18 - p. 11, l. 4, *citing* Doggett, col. 9, ll. 1-11, 19-23). A PCMCIA card for a workstation is clearly different than the smart card described in the claims. Moreover, because the PCMCIA card in Doggett is coupled to a workstation, there does not appear to be anything equivalent to the smart card communication device of the claims.

Claims 1, 17, 21, 22 and 29 describe the secure data exchanged between the smart card and the central computer system. The secure data is formatted by the smart card to allow the central computer system to detect a modification to the secured data occurring during transmission, beginning at the smart card and extending through to the remotely located central computer system. This particular form of end-to-end data integrity for a contactless smartcard is not taught or suggested by the references. The end-to-end processing, from smart card, *passed through* a smart card communication device, and to the remote central computer system, provides a mechanism to ensure that a secure packet has not been modified at any point between the smart card and the central computer system (including the smart card communication device). This end-to-end processing allows the smart card to send a packet to the central computer system to process a transaction without requiring intermediate network elements (e.g., the smart card communication device) to further interpret the *content* of that packet. Thus, in certain embodiments, the contents of the packet need "not [be] deciphered, decoded or authenticated anywhere within the communication link except at the smart card 106 and the

smart card server 130" located in the central computer system 102 (Original Application, p. 10, ll. 7-9).

Independent claims 17, 18 and 25 further set forth embodiments wherein, for transmission in the opposite direction, a smart card may detect a modification to the secured data beginning at the central computer and extending through to the smart card. Again, the central computer system is located remotely from the smart card and/or the smart card communication device.

Doggett: The Office appears to rely on Doggett to suggest the end-to-end data integrity of the claims. But, as noted above, the Office seems to equate the PCMCIA card and workstation of Doggett with the smart card and smart card communication device of the claims (Office Action, p. 3, ll. 17-22, *citing* Doggett, col. 9, ll. 1-11, 19-23). However, the distinctions between a PCMCIA card and a smart card are specifically set forth even in Doggett (Doggett, col. 14, ll. 4-19). The aspects of Doggett which may suggest end-to-end data integrity are described with specific reference to the PCMCIA card implementation (Doggett, col. 14, l. 20 - col. 16, l. 6). The PCMCIA card implementation is distinguished from other implementations.

For example, in Doggett, the PCMCIA card is coupled with the user's workstation for use on a more permanent basis, and these concepts are clearly different than the smart card and smart card communication device of the claims. The claims set forth, instead, the RF connection between smart cards and a smart card communication device. The smart card and smart card communication device of the claims have a number of different security issues than the PCMCIA card and user workstation of Doggett. Moreover, it is evident the generation of secure data on a contactless smart card is quite a different proposition than generating a digital signature via a PCMCIA card coupled with a workstation. Doggett itself makes these distinction clear.

It is also worth noting that in claims 17, 18, and 25, a second set of secured data is formatted to allow the smart card to detect a modification occurring during transmission beginning at the remote central computer system and extending to the smart card. This end-to-end data integrity in the opposite direction is not suggested in Doggett.

Hohle: The Office Action also appears to rely, at least tangentially, on Hohle to teach these limitations (Office Action, p. 3, ll. 2-10; p. 6, l. 13; p. 7, l. 14, *citing* Hohle, col. 22, ll. 47-67). But the cited portions of Hohle address "'signing' of the data using a message authentication code" for transmission between the "card" and "external device" (Hohle, col. 22, ll. 50-57). This "signing," however, falls far short of the end-to-end connectivity of the claims. The use of the MAC in Hohle is to authenticate content only between the card and an "external device," and there is no indication as to what device(s) constitute an external device. This clearly differs from the claims, which describe end-to-end data integrity between the smart card, *through* the smart card communication device, and to the remote central computer system. The central computer system in certain embodiments is configured to process a transaction for the smart card using the data formatted by the smart card.

The Office Action indicates that it is the issuer 10 of Hohle that reads on the central computer system of the claims (Office Action, p. 3, *citing* Hohle Fig. 10). But there is simply no suggestion that the use of the message authentication code for "signing" data be from the smart card to that issuer 10. There is no teaching or suggestion that the "external device" of Hohle is the issuer 10. The use of a message authentication code between a card and an intermediate device, as suggested by Hohle, clearly falls short of the end-to-end data integrity of the claims. The Office Action also attributes certain central computer system functions to the access point in Hohle (Office Action, p. 3, ll. 2-5). But the access point in Hohle is described as a card reader for interfacing with a smart card, and thus is different than the remote central computer system of the claims.

The Office Action further relies on Hohle to teach certain encryption and authentication for a smartcard system. While Hohle may describe user "authentication" and data "encryption," there is no teaching or suggestion of the claimed end-to-end form of data integrity beginning at the smart card and extending through to the central computer system. Hohle fails to describe the functionality of the system to "detect a modification to the secured data" throughout the transmission in the manner set forth in the claimed embodiments.

Implicitly, the Office admits that Murphy, Hilton, and Zuk fall short of teaching this limitation as well. Because it is asserted that the cited references do not teach the limitations

at issue, it is respectfully submitted that independent claims 1, 17, 18, 21, 22, 25, and 29 are allowable. Claims 2, 4-16, 20, 23, 24, 26, 27, 30-35, and 59 each depend from the independent claims, and these claims are believed allowable for at least the same reasons as given above. Applicants, therefore, respectfully request that the rejections under 35 U.S.C. 103(a) be withdrawn.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,

/Michael L. Drapkin/

Michael L. Drapkin
Reg. No. 55,127

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300

MLD:klb
60952631 v1